Tokyo 2020 col riconoscimento facciale (quello che piace al ministro Bongiorno per i furbetti della PA)

Per rendere le Olimpiadi di Tokyo 2020 più sicure gli organizzatori e le autorità locali hanno deciso l'utilizzo del riconoscimento facciale per tutti i protagonisti dei giochi, ad esclusione del pubblico. Sarà la prima volta nella storia che la tecnologia sarà utilizzata per un evento del genere. Come funziona? Badge più scansione del viso per atleti, staff, organizzatori e giornalisti per accedere nei diversi luoghi della città in cui si svolgeranno i giochi. Il sistema, già collaudato dal Giappone durante i Giochi di Rio del 2016 per i giornalisti accreditati alla Japan House, non fa altro che confrontare la foto archiviata nel momento dell'accreditamento con quella che viene scattata quando una persona passa davanti alla colonnina con l'occhio elettronico. I test hanno dato risultati positivi: *"Il sistema si è dimostrato 2 volte e mezzo più veloce di quello tramite codici a barre o controlli visivi",* ha detto **Masaaki Suganuma** vicepresidente della **NEC corporation**, la società che metterà a disposizione l'infrastruttura tecnologica per effettuare il riconoscimento attraverso la rilevazione biometrica. Infatti il sistema NeoFace, che vanta tra i suoi clienti il dipartimento di Sicurezza interna statunitense e la polizia di Chicago, è in grado di riconoscere anche atleti di due metri o sulla sedia a rotelle, perché verrà impiegata anche per le Paralimpiadi.

Problema privacy?

La tecnologia sarà utilizzata solo come misura di sicurezza per le persone direttamente coinvolte nell'evento, pubblico escluso, e il comitato olimpico registrerà le immagini dei

volti e li archivierà in un database a cui il sistema può accedere per la verifica. *“La tecnologia è accurata al 99.7%”,* ha spiegato il numero 2 della società NEC, non al 100% perché il sistema di riconoscimento basato sull’intelligenza artificiale fa ancora fatica a identificare persone di colore. Se si dovesse riscontrare questo problema allora il riconoscimento verrà effettuato da un essere umano addetto alla sicurezza.

Sistemi di rilevazione biometrica delle presenze contro i furbetti della PA in Italia?

Lo stesso sistema di rilevazione biometrica che verrà utilizzato a Tokyo 2020 piace anche al ministro della Pubblica amministrazione **Giulia Bongiorno**, che ha preso l’impegno di iniziarlo ad impiegare contro i furbetti della PA. *“È intenzione del governo”,* ha detto la ministra, “*prevedere l’obbligo di sistemi di rilevazione biometrica delle presenze che già sono stati sperimentati con risultati lusinghieri”,* ha detto il ministro alla Camera il mese scorso.

Problema privacy?

*“Sono compatibili con la legge sulla **Privacy**”* ha fatto subito sapere Bongiorno.

È vero.

Il sistema è a prova di privacy come dimostra il S. Giovanni di Dio e Ruggi D’Aragona nel Salernitano, il primo ospedale a utilizzare le impronte digitali per i dipendenti. *Key4biz* ha intervistato il direttore generale: “Impronte digitali anti-furbetti, nel nostro ospedale funzionano”.

Chissà se il ministro Giulia Bongiorno riuscirà nell'impresa *olimpica* di installare il riconoscimento facciale nella PA italiana.

The post Tokyo 2020 col riconoscimento facciale (quello che piace al ministro Bongiorno per i furbetti della PA) appeared first on Key4biz.

https://www.key4biz.it/tokyo-2020-col-riconoscimento-facciale-quello-che-piace-al-ministro-bongiorno-per-i-furbetti-della-pa/229273/

Cyberattacco a Mattarella, procura di Roma indaga per attentato alla libertà del capo dello Stato

Il cyberattacco a **Sergio Mattarella** ha rappresentato un tentativo di esercitare una pressione politica, dai toni eversivi, sul presidente della Repubblica. Per questo motivo la procura di Roma ha aperto un'inchiesta ipotizzando i reati di *'Attentato alla libertà del Presidente della Repubblica'* e di *'offesa all'onore e al prestigio del Capo dello Stato'*. Parallelamente indaga il **Copasir** (Comitato parlamentare per la sicurezza della Repubblica) che oggi ha ascoltato intorno alle 14:30 (non alle 13 come indicato nella convocazione) **Alessandro Pansa**, il Direttore generale del Dipartimento delle Informazioni per la Sicurezza (**DIS**). L'audizione non è stata trasmessa in diretta streaming e dalla

segreteria del Copasir ci hanno detto: *“è segreta e al termine ci sarà solo una comunicazione dell’orario di inizio e fine dell’audizione al direttore Pansa”.*

L’indagine della Procura di Roma. Tweet riconducibili ad un’unica origine

L’indagine della Procura di Roma, coordinata dal procuratore aggiunto **Antonio Racanelli** e dal pm **Eugenio Albamonte** (reati informatici e antiterrorismo), è stata avviata alla luce dell’informativa della polizia postale. Nel procedimento si ipotizza anche il reato di sostituzione di persona in relazione agli oltre 400 profili Twitter, tutti riconducibili ad un’unica origine, comparsi sui social network la notte tra il 27 e il 28 maggio scorso. Da quei profili partirono migliaia di messaggi di insulti e inviti alle dimissioni nei confronti della prima carica dello Stato.

Indagano anche la Polizia Postale e l’Intelligence sul tweetstorm #Mattarelladimettiti

La Polizia Postale e l’Intelligence indagano sulla creazione in pochi minuti di oltre 400 profili **Twitter**, nella notte tra il 27 e il 28 maggio scorso quando il Colle disse no a Paolo Savona come ministro dell’Economia nel governo M5S-Lega, per chiedere le dimissioni del Capo dello. Secondo le prime descrizione investigative il primo account creato sarebbe nato non a Mosca, come ipotizzato in un primo momento, ma sullo “snodo dati” di Milano. Inoltre gli inquirenti seguono su un’unica cabina regia (probabilmente italiana) dietro all’hashtag #MattarellaDimettiti.

The post Cyberattacco a Mattarella, procura di Roma indaga per attentato alla libertà del capo dello Stato appeared first on Key4biz.

https://www.key4biz.it/cyberattacco-a-mattarella-procura-di-roma-indaga-per-attentato-alla-liberta-del-capo-dello-stato/229151/

Phishing, ‘c’è un rimborso per te di 1.482 euro’. Agenzia Entrate ‘Una truffa’

Non a caso è stata escogitata in questo periodo dell’anno la truffa via email di false notifiche di rimborsi fiscali. Milioni di cittadini hanno appena terminato la dichiarazione dei redditi e in molti hanno ricevuto sulla posta elettronica una falsa comunicazione: ‘c’è un rimborso per te di 1.482 euro da parte dell’Agenzia delle Entrate’.

Nell’ultimo tentativo di phishing, che contiene il logo dell’Agenzia, si informa di un presunto tentativo di rimborso non andato a buon fine e si invita ad accedere al proprio portale per elaborare manualmente la procedura. A tale scopo, viene chiesto di aggiornare le informazioni del proprio account accedendo a un link contenuto nel testo della e-mail. Di seguito un esempio del messaggio:

Il messaggio proviene apparentemente da un indirizzo di posta dell’Agenzia (ad esempio noreplys221@agenziaentrate.gov.it o noreplys22@agenziaentrate.gov.it, ma è in realtà inviato da un mittente diverso, non riconducibile all’Agenzia delle Entrate. I messaggi di posta elettronica segnalati nascondono un evidente tentativo di entrare in possesso di informazioni riservate. Per evitare danni al proprio pc, l’Agenzia, totalmente estranea all’invio di queste comunicazioni, invita a non dare seguito al contenuto delle stesse e a cancellare immediatamente le false e-mail. L’Agenzia delle Entrate non invia comunicazioni via e-mail relative ai rimborsi; sul sito internet www.agenziaentrate.gov.it nella sezione *Come sono pagati i rimborsi*, si possono consultare le modalità corrette per ricevere un rimborso fiscale.

Come sono pagati (davvero) i rimborsi dall’Agenzia delle entrate

Che si tratti di un tentativo di phishing lo dimostra anche il fatto che l’agenzia delle Entrate non invia comunicazioni via email relative ai rimborsi. L’Agenzia delle Entrate, una volta riconosciuto il diritto al rimborso, dispone la restituzione delle somme secondo le modalità indicate dal contribuente e in base all’importo da pagare.

Accredito su Conto corrente

Se il contribuente ha fornito all'Agenzia delle Entrate le coordinate del suo conto corrente bancario o postale, il rimborso, qualunque sia l'importo, viene accreditato su quel conto. Ovviamente, in questo caso, è necessario che il beneficiario del rimborso coincida con l'intestatario (o uno degli intestatari, in caso di conto corrente cointestato) del conto corrente. In caso contrario, il rimborso non viene accreditato.

La comunicazione delle coordinate bancarie o postali presso cui si desidera l'accredito dei rimborsi può essere effettuata in ogni momento presso qualsiasi ufficio dell'Agenzia delle Entrate o attraverso l'applicazione disponibile sul suo sito internet. Chi è già registrato ai servizi telematici dell'Agenzia ed è in possesso, quindi, del codice Pin, può effettuare la richiesta di accredito attraverso il canale Fisconline.

I dati necessari per erogare i rimborsi sono: il codice Iban (*International Bank Account Number*) e, per i versamenti internazionali, il codice Bic (*Bank Identifier Code*) o Swift.

Altre modalità di accredito

Se non sono state fornite le coordinate del conto corrente bancario o postale, il rimborso viene erogato con modalità diverse a seconda della somma da riscuotere:

- per gli importi fino a 999,99 euro, comprensivi di interessi, il contribuente riceve un invito a presentarsi in un qualsiasi ufficio postale presso il quale, esibendo un documento d'identità, può riscuotere il rimborso in contanti. Chi si presenta in qualità di delegato, insieme alla delega compilata in ogni sua parte, deve esibire anche il documento d'identità del

delegante

- per gli importi oltre 999,99 euro e fino a 51.645,69 euro, comprensivi di interessi, al contribuente arriva un invito a comunicare le coordinate del proprio conto corrente, unitamente a un modello da compilare e consegnare, entro il termine indicato, a un ufficio postale. Se il contribuente non consegna il modello e non fornisce le coordinate del proprio conto, il rimborso viene eseguito con l'emissione di un vaglia della Banca d'Italia
- per gli importi superiori a 51.645,69 euro, comprensivi di interessi, e per i rimborsi di soli interessi di qualsiasi importo, la restituzione avviene, per ragioni di sicurezza, esclusivamente tramite accredito su conto corrente bancario o postale.

The post Phishing, 'c'è un rimborso per te di 1.482 euro'. Agenzia Entrate 'Una truffa' appeared first on Key4biz.

https://www.key4biz.it/phishing-ce-un-rimborso-per-te-di-1-482-euro-agenzia-delle-entrate-una-truffa/228709/

Cybersecurity, il piano del ministro Trenta 'Così combattiamo la guerra cibernetica'

L'Italia come può difendersi dalla nuova guerra in atto, quella cibernetica? *"Con la resilienza e il dual use*", queste sono le due parole chiave della strategia messa in campo dal ministero della Difesa, guidato da **Elisabetta Trenta.**

Resilienza e duplice uso affinché la Difesa non sia considerata più solo uno strumento militare, bensì un vero e proprio Sistema: integrato, connesso e a più livelli.

Il ministro, nell'illustrare alle Commissioni congiunte di Camera e Senato le linee programmatiche del Dicastero, ha spiegato come cambia la mission della Difesa proprio per fronteggiare le nuove minacce cyber. Dall'ultimo decennio a oggi, ha spiegato Trenta, alla Difesa viene sempre più chiesto di mettere a disposizione degli altri ministeri le proprie competenze e capacità per lo svolgimento di compiti non militari, proprio nell'ambito più ampio del concetto di resilienza.

"Le nuove minacce che ci troviamo di fronte esigono questo tipo di preparazione e il mio lavoro, in questo senso, sarà finalizzato a rendere l'Italia un Paese più sicuro sotto ogni aspetto, incluso il campo cibernetico" ha detto il ministro Trenta.

"Con resilienza", ha spiegato, *"mi riferisco alla capacità di adattamento dell'intero apparato statale, quindi di resistere e reagire a tutto ciò che possa turbarne la sicurezza, la*

stabilità interna e la governabilità attraverso l'opera concorsuale delle attività che ricadono principalmente nell'ambito delle aree di competenze dei vari ministeri a supporto del Presidente del Consiglio nella sua veste di Autorità Nazionale per la Sicurezza".

"Dual Use", invece, ha specificato il numero uno della Difesa *"intesa come la consapevolezza di dover sostenere, e al contempo ampliare, le opportunità di duplice uso delle capacità della Difesa per scopi non militari e a supporto, appunto, della resilienza stessa".*

La cyber defence centrale nell'azione di Governo

Nella prima occasione di "dialogo" col Parlamento il ministro della Difesa ha spiegato in che modo la cyber defence è e sarà centrale nell'azione di Governo:

"La minaccia cyber è un imprescindibile fattore di rischio per il Paese ma anche di grandi opportunità di investimento, aumentando il nostro grado di difesa e sicurezza. In linea con il processo di sviluppo delle tematiche di Cyber Defense in

ambito NATO e in generale con i programmi di 'trasformazione digitale', la Difesa ha già delineato le esigenze operative per rafforzare la sicurezza dello spazio cibernetico. In particolare, sono stati avviati una serie di programmi di acquisizione per accedere a strumenti operativi ad alto contenuto tecnologico in grado di assicurare la protezione, la resilienza e l'efficienza delle reti e dei sistemi informativi gestionali e operativi della Difesa", ha spiegato il ministro Trenta, che ha evidenziato la forte necessità di continuare ad investire nelle tecnologie di ultima generazione per combattere efficacemente la cyber guerra: "*In tale quadro, è necessario continuare ad investire, al fine di potenziare ulteriormente le dotazioni strumentali e organizzative di protezione cibernetica e sicurezza informatica, incrementando progressivamente la capacità di contrastare in maniera efficace le minacce. Le linee programmatiche del Ministero della Difesa 20". "È poi imprescindibile il conseguimento di capacità operative che andranno a supportare il neocostituito Comando Interforze per le Operazioni Cibernetiche (**CIOC**)",* ha dichiarato il ministro.

Le altre 'armi' in campo

Inoltre, ha annunciato Trenta, sarà promossa la pianificazione e l'implementazione di una vera e propria Strategia Nazionale Sistemica per il potenziamento della Sicurezza Collettiva e della Resilienza Nazionale, da sviluppare attraverso la collaborazione fra Ministeri, ma anche con l'Industria, l'Accademia, la Ricerca e il settore privato.

“Vogliamo che il concetto di ‘difesa’ che conosciamo diventi un vero e proprio Sistema e si inserisca nel concetto di sicurezza collettiva dell’intero Sistema-Paese, nel cui ambito gli altri Dicasteri condividano le proprie capacità nell’esclusiva tutela degli interessi nazionali” ha concluso il Ministro.

The post Cybersecurity, il piano del ministro Trenta ‘Così combattiamo la guerra cibernetica’ appeared first on Key4biz.

https://www.key4biz.it/cybersecurity-il-piano-del-ministro-trenta-cosi-combattiamo-la-guerra-cibernetica/228619/

mBanking, perché il tuo smartphone può mettere a rischio i tuo soldi

Lo smartphone rischia di essere la prima porta d'ingresso per i malintenzionati al nostro conto bancario. E' quanto emerge da un'indagine di due anni fa della **FED**, secondo cui la metà degli utenti smartphone di conti bancari ha utilizzato il telefonino per accedere ai suoi soldi.

Perché preoccuparsi? Perché secondo un'indagine della **Federal Trade Commission** americana, già 10 anni fa il furto d'identità era la prima causa di lamentela da parte degli utenti, e oggi il numero di lamentele per lo stesso motivo sono cresciute del 20%.

Nel 2017, secondo dati diffusi dalla società di advisory **Javelin Strategy & Research**, si sono registrati 17 milioni di furti d'identità. I data brach oggi riguardano in larga misura i nostri smartphone. E ovviamente il rischio di subire un furto di denaro sul nostro conto bancario tramite mobile device cresce di pari passo con l'incremento dell'mBanking e del numero di smartphone in circolazione. Di seguito alcune indicazioni su come come agiscono gli hacker e alcuni consigli per difendersi.

- **Phishing**. Quando gli hacker ti inviano mail e messaggi per carpirti informazioni sui tuoi dati personali. Una pratica vecchiotta, che diventa però sempre più sofisticata perché i siti degli hacker che ti attirano in trappola sembrano veri a tutti gli effetti. Secondo i

dati dell’**Anti-Phishing Working Group**, a fine 2016 gli attacchi phishing erano aumentati del 5.700% in 12 anni.

- **Keylogger software**. Si tratta di app non sicure che si installano sullo smartphone, magari non provenienti da un app store ufficiale. Il software maligno registra le battiture sullo smartphone, quando ad esempio accedi ad un conto bancario o ad un sito, e poi trasmette la registrazione all’hacker.

Come proteggersi

- **Informati con la tua banca sulle misure di sicurezza.** Le maggiori banche utilizzano protocolli di cybersecurity per proteggere il tuo conto da data breaches, furti di danaro e furti ad ampio raggio di identità personali.
- **La tua banca dovrebbe fornirti un’autenticazione a due fattori.** Quando cerchi d accedere al tuo conto online, la tua banca dovrebbe inviarti una richiesta di conferma del tuo tentato accesso attraverso un altro canale, magari un sms, per avere la conferma del login in corso. Non tutte le banche lo fanno, ma quelle che lo fanno sono certamente più sicure.
- **Alert delle transazioni.** Chiedi l’invio di almeno tre alert in caso di prelievi rilevanti in danaro oppure in caso del calo del conto sotto una certa soglia.
- **Monitoraggio delle frodi**. Molte banche controllano le transazioni per scoprire comportamenti di acquisto inusuali. Ad esempio, la banca potrebbe inviarti un sms di conferma per un acquisto di una somma insolita rispetto alla media oppure quando riscontra una strana richiesta di acquisto mai vista prima. Prima di chiudere la transazione dovresti dare conferma alla banca.
- **Aggiornare i software del tuo smartphone.** Ricordarsi di installare le versioni più aggiornate dei software di protezione.

- **Password, sceglierla lunga e complicata.** Così, anche se perdi lo smartphone chi lo troverà non riuscirà ad accedere al tuo conto. Inoltre, usa una password complessa per bloccare il telefonino.

The post mBanking, perché il tuo smartphone può mettere a rischio i tuo soldi appeared first on Key4biz.

https://www.key4biz.it/mbanking-perche-il-tuo-smartphone-puo-mettere-a-rischio-i-tuo-soldi/228579/

‘Bene la Direttiva NIS, ogni azienda comprenda il suo modello ideale’. Intervista ad Andrea Chittaro (neo Presidente AIPSA)

La sicurezza informatica ha ormai un ruolo centrale all’interno di ogni contesto aziendale, in particolar modo per la protezione delle infrastrutture critiche, dove investimenti sempre più grandi per far fronte al crescente numero di violazioni, portano le aziende a concentrare la sicurezza nelle mani di Chief Security Officer esperti. **Key4biz** ha intervistato **Andrea Chittaro,** *Head of Global Security & Cyber Defence Department* presso **Snam**, la principale utility del gas in Europa, nominato di recente Presidente dell’Associazione dei Professionisti della Security Aziendale (**AIPSA**).

Key4biz. ***Quanto è importante la sicurezza e la protezione***

delle infrastrutture critiche al giorno d'oggi?

Andrea Chittaro. E' importante perché queste infrastrutture forniscono "servizi essenziali" al paese ai cittadini, come sottolineato dalla più recente definizione proposta dalla **Direttiva NIS.** Attendiamo ora la concreta applicazione della Direttiva del 2008 sulle Infrastrutture Critiche Europee che prevede, tra l'altro, l'introduzione della figura del "*Security Liaison Officer*". Nel frattempo hanno preso il via diverse iniziative di partenariato pubblico-privato, altre sono state rinnovate e/o consolidate. C'è una crescente consapevolezza della necessità di fare "sistema" anche in Italia.

Key4biz. ***Purtroppo ancora sono poche le aziende che hanno nel proprio organico una figura con una responsabilità specifica come la sua. Quali sono oggi le principali sfide per il CSO?***

Andrea Chittaro. La prima e più importante è sul piano culturale. C'è una grande necessità di far comprendere sempre più il valore aggiunto tangibile di un approccio "olistico" alla Security, cioè di creare strutture che includano tutti i domini verticali della sicurezza. Ciò e' essenziale in un'epoca dove la distinzione tra spazi fisici e logici non ha più cittadinanza. Solo da una visione complessiva possono nascere opportunità per la creazione di valore che poi è lo scopo principale dei singoli business. La figura del CSO deve diventare il riferimento unico sulla gestione del rischio di security delle proprie aziende.

Key4biz. ***Il 16 maggio scorso è stato approvato in Consiglio***

dei Ministri il Decreto Legislativo per attuare in Italia la Direttiva NIS entrata in vigore il 26 giugno. Ritiene che adesso l'attuale quadro normativo e gli ambiti di applicazione previsti dal Decreto garantiscano un adeguato livello di protezione?

Andrea Chittaro. Il quadro normativo ha un'utile funzione di indirizzo. Ma è l'azienda che deve poi sottoporsi ad una sorta di "autodiagnosi" per comprendere dove si posiziona in un'ideale modello di sicurezza. Significa ritagliare su se stessa ed il proprio modello di business la soluzione di governance ed operativa più confacente. E' un lavoro a volte lungo ed anche complesso. La sicurezza deve seguire percorsi virtuosi e prevedere investimenti adeguati. Se tutto questo viene affidato a dei professionisti della Security Aziendale i benefici sono assicurati.

Key4biz*.Alle aziende spetta un ruolo fondamentale per migliorare la sicurezza e la protezione in ambito cyber delle proprie strutture, ma è altrettanto fondamentale la cooperazione con il pubblico. Come si vorrà muovere L'AIPSA a tale riguardo?*

Andrea Chittaro. AIPSA intende porsi come interlocutore autorevole e privilegiato per Istituzioni e Stakeholders nel processo di definizione delle migliori politiche di sicurezza, sull'asse pubblico-privato, nell'interesse preminente del sistema paese. Rappresentiamo molte delle più grandi aziende italiane e pensiamo di poter portare un contributo qualificato al dibattito su questi temi. Oltre a questo ci siamo dati come obiettivo quello di formare la "Next Generation" dei Security Manager. Che è la sfida che più mi appassiona.

The post ‘Bene la Direttiva NIS, ogni azienda comprenda il suo modello ideale’. Intervista ad Andrea Chittaro (neo Presidente AIPSA) appeared first on Key4biz.

https://www.key4biz.it/bene-la-direttiva-nis-ogni-azienda-comprenda-il-suo-modello-ideale-intervista-ad-andrea-chittaro-neo-presidente-aipsa/227253/

App e geolocalizzazione, il 60% degli italiani teme per la propria privacy

Gli utenti sono sempre più preoccupati rispetto a quanto possano essere osservate le loro attività su internet e alla possibilità di essere rintracciati grazie ai segni lasciati dai percorsi fatti online.

In un recente sondaggio condotto da **Kaspersky Lab** è stato rilevato che il **60,2%** delle persone non si sente a proprio agio nel condividere informazioni sulla propria posizione con i siti web e le applicazioni, una percentuale in aumento rispetto a quanto rilevato nel 2016 (all’epoca pari al **50,6%**).

Inoltre, quasi la metà degli utenti (il **50,3%**) dichiara una certa preoccupazione per la possibilità che qualcuno possa osservare tutte le attività fatte o i contenuti visti sui propri device; una percentuale simile di utenti, il **51,2%**, dichiara di aver paura del fatto che qualcuno possa rintracciarli usando le informazioni di geolocalizzazione.

Preoccupazioni fondate?

Gli esperti hanno scoperto che le app non solo possono aver accesso ad un'enorme quantità di dati (anche di una certa importanza, come la posizione di un utente, le informazioni circa i suoi contatti, le sue attività e molto altro), ma che lavorano spesso in background all'insaputa degli utenti stessi. Secondo la ricerca globale dal titolo "*My precious data*" condotta sempre dall'azienda russa, l'**83%** delle app Android ha accesso ai dati sensibili dei proprietari e il **96%** di queste stesse app può essere avviato senza alcun consenso. Queste preoccupazioni possono comunque essere evitate adottando alcune semplici misure di sicurezza.

Gli utenti dedicano poca attenzione alla sicurezza

Nonostante tutto questo, le persone non prestano abbastanza attenzione alla sicurezza dei propri dati o alle misure per tutelare la propria privacy, accorgimenti che, invece, potrebbero aiutare a farle stare più tranquille – per esempio, il **35,3%** degli utenti coinvolti dal sondaggio ammette di non controllare le autorizzazioni delle app preinstallate sui propri dispositivi Android e iOS, e il **10,6%** di loro dichiara di non effettuare il controllo nel corso del download o dell'installazione di nuove app. Per questo gli utenti, pur essendo sempre più preoccupati, restano comunque senza protezione rispetto alla possibile perdita dei loro dati.

Come proteggersi

Ecco allora 5 consigli su come proteggersi al meglio la

propria privacy.

- Uscite dalla sessioni di Twitter, Facebook e Gmail prima di disconnettervi
- Non connettetevi a reti WIFI pubbliche non protette
- Verificate l'autenticità di siti web e app
- Settate un Google Alert sui vostri dati personali
- Nascondete la vostra posizione

The post App e geolocalizzazione, il 60% degli italiani teme per la propria privacy appeared first on Key4biz.

https://www.key4biz.it/app-e-geolocalizzazione-il-60-degli-italiani-teme-per-la-propria-privacy/227206/

Cybersecurity Act, Parlamento Ue approva misure per rafforzare l'ENISA e creare sistema di certificazione unico

Nuovo passo in avanti per la **riforma della cyber sicurezza in Europa**, con le nuove misure approvate dalla Commissione Industria, ricerca ed energia del Parlamento europeo (o **Commissione ITRE**) su cui lavorare nei prossimi mesi per giungere ad un quadro normativo generale più attuale e soprattutto più efficace.

Ad ottobre del 2017, il **Consiglio europeo** ha chiesto

l’adozione di un approccio comune in materia di cyber sicurezza nell’Unione europea (Ue) in seguito al pacchetto di riforme proposto dalla Commissione. È partito da qui l’iter parlamentare della riforma che martedì la Commissione ITRE ha ulteriormente rilanciato con la proposta di quattro nuove iniziative: una **più forte Agenzia Ue per la sicurezza delle reti e dell’informazione (ENISA)**; **dispositivi, applicazioni e apparecchi per l’Internet of Things per più sicuri** per i cittadini dell’Unione (tra cui gli elettrodomestici e gli apparecchi elettrici della smart home); ridurre il più possibile rischi e minacce per le informazioni e le reti nell’Ue; migliorare e potenziare la **cyber resilienza**.

Più in generale, la Commissione ha approvato una misura generale per lavorare all’istituzione di **sistemi di certificazione comune a livello di UE per prodotti, servizi e processi ICT**.

In tal modo, gli eurodeputati intendono garantire e certificare che un prodotto o un servizio dell’*Information and communication technology* al momento del rilascio non

presentino nessuna vulnerabilità nota e che siano conformi agli standard e le specifiche tecniche internazionali.

I sistemi di certificazione consisterebbero in norme, prescrizioni tecniche e procedure. Il loro ruolo sarebbe quello di ridurre la frammentazione del mercato ed eliminare gli ostacoli normativi, instaurando al tempo stesso un clima di fiducia. Sarebbero riconosciuti in tutti gli Stati membri, facilitando così gli scambi transfrontalieri delle imprese.

In linea di massima la certificazione sarà rilasciata su base volontaria, ma non è esclusa "l'obbligatorietà della prova" in alcuni casi considerati critici e di particolare rilevanza in termini di sicurezza dell'Unione.

La nuova bozza di riforma approvata in Commissione ITRE due giorni fa ha l'obiettivo anche di rafforzare l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA).

Con un mandato permanente, sottolinea la commissione ITRE nella sua posizione, l'ENISA potrà contare su maggiori risorse economiche, oltre che su uno staff più vasto, distribuito tra le sedi di Candia e Atene. Inoltre, l'Agenzia diventerà il punto di riferimento per il quadro europeo di certificazione della cibersicurezza per i prodotti e servizi ICT, con un sito web apposito che raccoglierà tutte le informazioni sulle certificazioni adottate nell'Ue.

La cibersicurezza può consentire il raggiungimento di un più alto livello generale d'innovazione e contribuire allo sviluppo dell'economia dei dati. Dare sicurezza al futuro

digitale dell’Europa può significare anche affrontare le minacce alle piattaforme online e consentire loro di apportare un contributo positivo alla società; sostenere le piccole e medie imprese affinché siano competitive nell’economia digitale; investire nell’uso dell’intelligenza artificiale e dei supercomputer in settori quali le cure mediche e l’efficienza energetica.

La bozza della riforma sarà discussa durante la sessione plenaria di settembre e sarà il testo base su cui saranno avviate le negoziazioni con il Consiglio europeo.

The post Cybersecurity Act, Parlamento Ue approva misure per rafforzare l’ENISA e creare sistema di certificazione unico appeared first on Key4biz.

https://www.key4biz.it/cybersecurity-act-parlamento-ue-approva-misure-per-rafforzare-lenisa-e-creare-sistema-di-certificazione-unico/226966/

Il Pentagono punta sui giovani talenti della Silicon Valley per formare l’esercito del futuro

Recentemente è apparso su **Wired** un articolo che racconta le mosse del Pentagono per creare l’esercito cibernetico del domani. Non si tratta di un piano di investimenti per la ricerca di tecnologie futuristiche da implementare presso

l’esercito americano, si tratta piuttosto della testimonianza di come, investendo nei giovani e nelle loro attitudini/passioni (in questo caso giovani soldati), si possano raggiungere importanti traguardi – e costi ridotti – per la sicurezza nazionale.

Come valorizzare le capacità dei soldati appassionati di tecnologia

L’articolo Wired racconta la particolare mansione che lo US Army ha affidato a **Nicole Camarillo**, Executive Director, Talent Strategy e Special Operations Team presso lo US Army Cyber Command. Camarillo svolge un’importante lavoro di persuasione nei confronti del personale impiegato presso la Silicon Valley, al fine di convincerli a lasciare il proprio lavoro e approdare nello US army, esprimendo nell’esercito il proprio know how.

L’articolo raccontata la storia, verificatasi alcuni anni prima, di un giovane capitano chiamato con lo pseudonimo Matt che, avendo una forte attitudine verso l’informatica, si è occupato dello sviluppo di un tool utilizzato in Medio Oriente in grado di abbattere i droni nemici.

La storia del capitano Matt non è un caso isolato, l’idea non è soltanto quella di assumere ex dipendenti presso la Sylicon Valley, ma è soprattutto quella di selezionare personale militare con fronte attitudine – e passione – verso la tecnologia. A riprova di ciò viene riportata una partnership fra lo US Army Command e il Defense Digital Service (DDS). Si tratta di una sorta di start up originatasi all’interno del

Dipartimento della Difesa USA, il cui team leader Jyn Erso – nickname ispirato ad un personaggio della saga di Star Wars – ha portato a compimento alcuni progetti che prevedevano lo sviluppo di importanti tools da sfruttare in territorio nemico. Da notare è come precedenti tentativi di sviluppo dei medesimi tools presso i contractors, sono costati all'esercito americano centinaia di milioni di dollari e di insuccessi.

L'obiettivo per lo US Army, come detto, è stato inizialmente quello di attrarre le menti brillanti presenti nella Silicon Valley e convincerle a prendere servizio a Washigton, in modo tale da creare dei team che avessero la forma di start-up utili ad aggirare la "palude" della burocrazia militare. La finalità di tali gruppi è quella di creare, per conto dell'esercito, tecnologia userfriendly che non richieda anni di sviluppo e possibilmente un costo ridotto in termini di ricerca e sviluppo.

Sin dalla sua origine, avvenuta nel 2015, il DDS ha creato vari tools fra cui ~~un~~ alcuni strumenti in grado di tenere traccia delle attività svolte dai soldati in Afghanistan, sostituendo un precedente software sviluppato in sede NATO.

Come fa notare Wired, per anni nel settore militare la qualifica di "tecnico" è stata associata ad un soldato con profonde conoscenze nella meccanica dei carri armati, non a qualcuno con la capacità di scrivere software. Il caso del capitano Matt è emblematico: ha studiato ingegneria informatica, ha lavorato per la National Security Agency, si è successivamente formato come ranger ed è in servizio militare da oltre 7 anni. Tuttavia, tutte le volte che si è trattato di spostarlo di reparto, nessuno di questi prevedeva operazioni cibernetiche poiché l'esercito americano non ha sviluppato un

specifico settore fino al 2015.

Nicole Camarillo e **Chris Lynch,** quest'ultimo Director of US Defense Departiment's Defense Digital Service, vogliono dare ai soldati come Matt la libertà di creare e sperimentare, per conto dell'esercito americano, nel settore della cyber-security. Con questo obiettivo nel 2017 approcciarono il generale Paul Nakasone, fondatore del Commander of Cyber Army, con l'idea di trasferire per alcuni mesi un piccolo gruppo di soldati al Pentagono e lavorare assieme al DDS.

Nakasone, oggi capo della National Security Agency, trasferì quel personale in un progetto chiamato Jyn 1 (riferimento a Jyn Erso), che si prefiggeva di creare una tecnologia in grado di abbattere i droni nemici.

Il successo della scelta di Nakasone oggi è testimoniato dalla nascita di una Army Cyber School e dalla valorizzazione di alcuni soldati con la passione per la tecnologia. Wired documenta alcuni esempi: un tecnico dell'aeronautica con la passione per l'hacking delle macchine, oppure un soldato di Fort Maede con grandi capacità nella matematica e nella statistica. Porre in pratica l'idea per cui è possibile servire nell'esercito valorizzando ulteriori capacità dei soldati, ha fatto sì che si arruolassero altre personalità brillanti. Oggi, infatti, il DDS è composto da ingegneri, designer, project manager e altre figure professionali che hanno lasciato i propri lavori presso Facebook, Deloitte e Dropbox per lavorare al Pentagono.

Come detto, una delle prime questioni affrontate dal DDS,

riguardava la ricerca di uno metodo per fermare ISIS dal lanciare granate sui soldati sfruttando i droni. Cercare di risolvere questo problema ha portato l'esercito americano alla perdita di oltre 700 milioni di dollari. Sono stati utilizzati vari mezzi: si è provato a sparare, l'esercito francese si è avvalso di aquile addestrate nonché dell'utilizzo di strumenti che sfruttavano l'energia cinetica.

DDS riuscì a sviluppare, invece, una tecnologia che sfrutta le onde radio, risulta facile da trasportare ed è capace di non interferire con le comunicazioni circostanti. Inoltre, si preoccuparono di sviluppare un software upgradabile che fosse sempre aggiornato alle nuove tipologie di droni presenti sul mercato.

Un altro valore aggiunto apportato dal DDS è stata la modifica della metodologia di lavoro nel settore dello sviluppo tecnologico all'interno dell'esercito americano. Normalmente, infatti, un'azienda che vince un appalto per la costruzione di nuove tecnologie, riceve una serie di requisiti da soddisfare e procede al testing presso i propri laboratori. Ciò comporta che i soldati hanno accesso all'utilizzo della tecnologia in una fase tardiva dello sviluppo, comportando la scoperta di problematiche non inizialmente calcolate.

DDS invece introduce un ciclo di sviluppo assimilabile ad una software house, ovvero, il team prepara una build del prodotto, successivamente i soldati fanno il "beta testing" e, sulla base dei dati raccolti e delle esigenze dei soldati, DDS migliora il prodotto. Ciò permette sin dalle fasi iniziali di sviluppare tecnologia che risponde maggiormente alle necessità del campo di battaglia.

Tale logica è stata alla base dello sviluppo di Jyn 1, determinando un costo del progetto di circa 100 mila dollari, a fronte dei 700 milioni di perdite spese in contractors che non hanno raggiunto l'obiettivo.

Oggi il DDS ha modificato i suoi obiettivi, non solo effettua il recruit di personale presso la Silicon Valley, ma attualmente si concentra sulla "coltivazione" dei talenti già presenti presso le forze armate americane.

Così come sottolinea Wired, in un momento storico che richiede particolare attenzione verso il panorama dell'hacking sia dal punto di vista della sicurezza nazionale che della protezione degli asset strategici per il paese, diventa cruciale per l'esercito adattarsi alla realtà e prendere consapevolezza del campo in cui avviene il confronto, in questo caso quello cibernetico.

Nel corso delle ultime settimane si è parlato di vari successi da parte di gruppi State-sponsored cinesi, come nel caso di **Sea-Dragon**, dell'hacking di aziende che si occupano del controllo e della gestione di satelliti, nonché di **Winnti Umbrella**. Probabilmente bisogna considerare questa nuova idea in senno all'esercito americano come una risposta all'hacking di Stato cinese.

Ma quanto esposto, cosa insegna?

L’articolo è particolarmente interessante perché mostra come, quando si investe nelle attitudini e nelle passioni delle persone (ad esempio di un giovane), si possono trarre molteplici benefici che, in questo caso, vanno tutti a beneficio della sicurezza nazionale.

Non solo, gli esempi mostrati permettono di affermare come, se poste nella giusta condizione, le persone tendono a lasciare il posto di lavoro presso multinazionali – in cui potrebbero guadagnare di più – per lavorare al servizio della sicurezza dello Stato. Questo è molto importante in termini di cultura della sicurezza, ovvero nella scelta fra il guadagno “puro” e nell’avvertire la necessità di contribuire alla sicurezza di tutti.

Cambia inoltre la valutazione di utilità all’interno di un’organizzazione come l’esercito poiché si incrementa la consapevolezza di quanto un software possa determinare potenziali conseguenze sul campo esattamente quanto un’arma.

In conclusione, ritengo questa sia la giusta direzione che deve prendere l’Occidente in merito all’investire nella sicurezza nazionale.

Questo articolo è apparso originariamente su *Cybersecitalia.it*

The post Il Pentagono punta sui giovani talenti della Silicon Valley per formare l’esercito del futuro appeared first on Key4biz.

https://www.key4biz.it/il-pentagono-punta-sui-giovani-talenti-della-silicon-valley-per-formare-lesercito-del-futuro/226949/

Cybersecurity, 3,5 milioni di posizioni scoperte entro il 2021

Il cybercrime potrebbe diventare una grande opportunità di carriera per tutti i professionisti del settore, ma anche un'importante sfida per le aziende che dovranno saper affrontare questa carenza di personale qualificato.

Lo dicono i numeri di **Wyser (Gi Group)** che ha realizzato un'analisi del settore della cyber sicurezza e della privacy (GDPR 2018) e redatto una strategia rivolta alle aziende che riconoscono la rilevanza della sicurezza cibernetica e vogliono coltivare talenti al proprio interno affrontando al meglio questa sfida.

Vulnerabilità, malware, esposizione dei dati e, da poco, **GDPR** compliance. Sfide e preoccupazioni che riguardano le aziende di tutta Europa e non solo. Si stima infatti che il "cybercrimine" porterà a triplicare il numero di posizioni aperte nei prossimi cinque anni. Una grande sfida per le aziende, che a livello globale, lamentano una carenza di personale qualificato laddove, invece, i manager HR prevedono di far crescere il reparto dedicato del 15%.

Grande opportunità quindi per chi è in cerca di lavoro, anche perché la cybersecurity abbraccia ogni tipo di settore: se in testa troviamo i servizi professionali (37%), non mancano le richieste nel mondo della finanza (13%), della difesa (12%), ma anche della sanità (6%).

5 punti cardine per attirare professionisti qualificati in materia di Cybersecurity

- Formazione e aggiornamento continuo: *Prevedere piani di investimento strutturati per un costante aggiornamento del personale*
- Flessibilità nella ricerca e selezione: *Includere nella selezione anche candidati con background non strettamente tecnico*
- Misure di conciliazione vita-lavoro: *Garantire flessibilità di orario e altri benefit per rendere l'azienda più attrattiva rispetto ai competitor*
- Opportunità di carriera all'interno dell'azienda: *Dare alle risorse la possibilità di crescere all'interno dell'azienda evitando così un rapido turn-over*

- Diffusione di una cultura della cybersecurity in azienda: *Costruire una cultura della sicurezza informatica a tutti i livelli, riconoscendo il valore dello specialista*

Come attirare professionisti in materia di cyber sicurezza

Sono diversi gli studi e i profili che affollano questo settore: ingegneri, architetti delle informazioni, laureati in economia, giurisprudenza, criminologia o scienze politiche. Professionisti che si sono avvicinati a quest'ambito in un secondo momento, spesso per passione, e che hanno saputo accumulare esperienze dirette restando aggiornati con corsi di perfezionamento e certificazioni.

"L'87% degli esperti di cybersecurity, nel mondo, non ha iniziato la propria carriera in questo settore. Essere troppo rigidi nella scelta iniziale rischierebbe di far scartare a priori talenti che presentano una formazione alternativa a un percorso più tradizionale, ma non per questo meno valida", commenta" **Carlo Caporale, Amministratore Delegato Wyser Italia**.

Il settore della sicurezza informatica si contraddistingue per la rapidità con cui evolve in tempi molto brevi. Ne è una prova la recente introduzione della nuova regolamentazione in materia di privacy in Europa, la cosiddetta **GDPR 2018**. L'obbligo da parte delle aziende di adeguarsi a questa nuova normativa ha portato a prendere in seria considerazione l'inserimento in organico di personale specializzato, spesso

incrementando le risorse già dedicate.

“L’adeguamento delle aziende in seguito all’introduzione del nuovo regolamento in materia di privacy è un chiaro esempio della velocità con cui questo settore evolve”, continua **Caporale.** *Tutto ciò richiede da una parte che il professionista si aggiorni con costanza, anche quando ha raggiunto una posizione stabile, e dall’altra che l’azienda contribuisca alla sua continua formazione con piani di investimento strutturati: solo così potrà vincere la sfida di risultare attrattiva agli occhi di nuovi talenti e anche a quelli delle proprie risorse, per essere così vincente sul mercato ”.*

The post Cybersecurity, 3,5 milioni di posizioni scoperte entro il 2021 appeared first on Key4biz.

https://www.key4biz.it/cybersecurity-35-milioni-di-posizioni-scoperte-entro-il-2021/226313/